Self-reported motivations for engaging in or desisting from cyber-dependent offending and the role of autistic traits.

Katy-Louise Payne, Katie Maras, Richard Mills, Ailsa J Russell, Mark J Brosnan

Abstract

Cyber-dependent offending, i.e. criminal behaviour reliant on computing and the online domain, have been reportedly associated with particular characteristics and motivations such as being young, male, autistic and motivated by challenge. These associations are anecdotal however and empirical evidence is limited. The present study investigated reasons for engaging or declining to commit cyber-dependent offending in cyber-skilled non-offenders (n=175) and offenders (n=7) via an online survey measuring cyber-dependent criminality. The potential role of autism and autistic traits was also considered. Qualitative interviews about motivations for offending were carried out with the offenders. Twenty-nine (approximately 17%) of the non-offenders had been asked to engage in cyber-dependent offending but had declined. Their reasons and motivations for declining to commit cyber-dependent offences were compared with the cyber-dependent offenders reasons and motivations for engaging in cybercrime. Seven main reasons for declining to offend were identified: (1) moral principles; (2) perception of risk; (3) fear of consequences; (4) not wanting to; (5) wanting to adhere to the law; (6) behaviour being too complicated; and (7) price being too low. The cyber-dependent offenders reported seven main reasons for engaging in cyber-dependent offending: (1) lack of understanding; (2) entertainment; (3) peer influence; (4) experience and career; (5) anonymity and risk perception; (6) life events; and (7) morals. Implications for practice are discussed.

Keywords: offending; autistic traits; autism; cyber-dependent offending; cybercrime; motivations

What this paper adds

This paper contributes to our understanding of cyber-dependent offending and the previously hypothesised link to autism and autistic traits. This study is the first to explore the self-reported motivations for engaging in and declining to engage in cyber-dependent offending. These motivations are subsequently related to the level of autistic traits. This paper provides a starting point for both future research and the development of cyber-dependent offending prevention interventions.

Self-reported motivations for engaging in or desisting from cyber-dependent offending and the role of autistic traits.

1. Introduction

Cybercrime is defined as, "The illegal use of computers and the internet, or crime committed by means of computers and the internet" (Ledingham and Mills, 2015, p3). Within this, cybercrime is predominantly divided into two categories: cyber-enabled crime and cyber-dependent crime. Cyber-enabled crimes are 'traditional' crimes (such as fraud) that are not reliant on computer technology but can be upscaled through the use of a computer, computer network or other information communication technology (McGuire & Dowling, 2013; The National Crime Agency, 2016). Cyber-dependent crimes refer to crimes which cannot be committed without the use of a computer, computer network or other form of information communication technology (ICT), such as the creation and spread of malware, hacking, and denial of service attacks (McGuire & Dowling, 2013; National Crime Agency, 2016). In the year ending June 2017, cyber-dependent crime offences accounted for over one fifth of all reported offences in England and Wales, with 1.6 million computer misuse offences reported (1.1 million virus-related offences and 500,000 incidents of unauthorised access to personal information; Office for National Statistics, 2017). This is higher than more traditional crimes such as violence (1.24 million offences), burglary (667,000 offences), and robbery (132,000 offences; Office for National Statistics, 2017) and represents a growing threat and cost to the economy (National Crime Agency, 2016). Despite this, relatively little is known about cyber-dependent offenders, who are the focus of the current study.

Reports indicate that UK cyber-dependent offenders are typically male and young (National Crime Agency, 2017). For example, the average age of suspects and those ultimately arrested by the National Crime Agency Cybercrime Unit in 2015 was 17 years, compared to 37 years for drug offences (National Crime Agency, 2017). It has been

suggested that financial gain is not necessarily a priority for this group of young offenders but rather the sense of challenge and accomplishment are key drivers for their offending behaviour (National Crime Agency, 2017). Whilst this data is UK-based, the issues of cyber-dependent crime and this profile of offenders is consistent across a range of countries, including the UK, USA, Australia, New Zealand, Germany, the Netherlands, and Denmark (Ledingham & Mills, 2015).

There is a dearth of research regarding the reasons why individuals engage in cyber-dependent offending. One reason for the paucity of research into cyber-dependent offenders is that the cyber world is filled with blurred lines which may make it less obvious when an individual commits an offence. For example, although gaming modifications are technically illegal due to breaches of copyright, gaming vendors frequently promote this practice (CREST, 2015). Game modification is thought to be a gateway into cyber-dependent crime (National Crime Agency, 2017). Sotomaa (2010) suggests five key motivations for engaging in game modifications: (1) playing (e.g., having an idea and wanting to insert it into game); (2) contemporary manifestation of the hacker legacy (e.g., viewing the game as challenging code based system to be hacked); (3) researching (e.g., enthusiasm to clarify code details and the background of the subject matter); (4) artistic expression (e.g., games used to express individuals political views); and (5) cooperation (e.g., working with others). Some of the motivations for gaming modification (e.g., the hacker legacy) refer to skills which are not specific to gaming modifications. This may, in combination with the blurred lines between legal and illegal behaviours discussed above, help to explain the relative ease and unknowing with which individuals may find themselves committing cyber dependent offences.

There are a wide range of motivations reported for engaging in cyber-dependent crime, such as hacking into ICT systems. Hacker motivations are reported to include positive social reasons (i.e., socialising opportunities), negative social reasons (e.g., attention seeking,

revenge), intellectual gain, self-satisfaction (e.g., self-fulfilment, self-gratification), economic rewards and technologically positive reasons (e.g., opportunity to identify computer system weaknesses; Cayubit et al., 2017). This is consistent with the assertion from the National Crime Agency (2017) that motivations for cyber-dependent crime can be different from traditional crime (such as fraud for financial gain). Consistent with this, individuals engaging in cyber-dependent offending are unlikely to have engaged in traditional offline offending (National Crime Agency, 2017).

Another supposition by the National Crime Agency was that there could be a link between autism and cyber-dependent offending (National Crime Agency, 2017). In the absence of empirical evidence, Brosnan (in press) speculated that autistic traits, rather than autism, may relate to cyber-dependent crime. Autistic traits (e.g., social imperviousness, directness in conversation, lack of imagination, affinity for solitude, difficulty displaying emotions: Gernsbacher, Stevenson & Dern, 2017) are considered to exist on a continuum in the general population with autistic groups typically reported to have higher levels of autistic traits than non-autistic groups (Baron-Cohen et al., 2001; 2006; Constantino & Todd, 2003; Kanne et al., 2013; Plomin, Haworth & Davis, 2009; Posserud, Lundervold & Gillberg, 2006; Skuse et al., 2009; see also Bolte et al.,2011; Gernsbacher et al., 2017; Ronald & Hoekstra, 2011; Ruzich et al., 2015 for meta-analysis). Recent research is consistent with this assertion identifying relationship between autistic traits and cyber-dependent crime, but not autism and cyber-dependent crime (Payne et al., 2019; Seigfried-Spellar et al., 2015). Payne et al. (2019) report that autistic traits directly related to cyber-dependent crime and indirectly related to cyber-dependent crime mediated by a relationship with enhanced digital skills. Whilst autistic traits predicted cyber-dependent crime, a diagnosis of autism per se acted as a protective factor against cyber-dependent offending. This is interesting as typically autistic people have

higher levels of autistic traits than non-autistic people. Within the autistic group higher levels of autistic traits related to greater digital skills but not cyber-dependent crime.

In sum, the very limited information to date suggests the profile of cyber-dependent criminals to be teenage males with higher autistic traits who are engaging in cyber-dependent criminal activity for different motivations than traditional (offline) criminals; however, this remains to be empirically examined. Thus, this study aimed to: (1) explore the motivations for engaging in cyber-dependent offending; and (2) provide preliminary data on the autistic traits of both cyber-dependent offenders and individuals who decline to engage in cyber-dependent offending.

2. Method

2.1. Participants

One-hundred-and-seventy-five cyber-skilled non-offenders and seven cyber-dependent offenders completed an online survey measuring autistic traits and cyber-dependent criminality. Twenty-nine of the non-offenders (16.57%) reported that they had been approached to commit a cyber-dependent crime but had declined. Henceforth this group shall be referred to as the cyber-dependent decliner (CDD) group. The CDD group (n = 29) and the cyber-dependent offender (CDO) group (n = 7) form the basis of this paper.

The CDD group were composed of 16 males and 13 females with an average age of 28.59 years (range = 14-47; SD = 9.16). These individuals were recruited through various channels including the University of Bath computer science department and the Cyber Security Challenge; an organisation looking to promote the development of cyber-skilled individuals. We therefore targeted participants likely to have relatively high levels of computer-related skills.

The CDO group were all were male with a mean age of 18.29 years (range = 16-24; SD = 3.30). All CDO participants had committed offences categorised as Computer Misuse

Offences (e.g., unauthorised access to and/or modification of computer material; creating, supplying or obtaining anything which could be used to commit computer misuse offences). These individuals were all recruited via the National Crime Agency in the UK, who sent out letters to 67 CDOs with whom they had had contact within an official capacity. The letter provided information about the study and asked them to contact the researcher if they were willing to participate in the research. This obtained a response rate of approximately 10%. The exclusion criteria for this research were individuals: (1) under 14 years old; (2) those who had a head injury; or (3) those had untreated epilepsy. The age criteria were chosen because individuals aged 14 years or above are starting to tailor their education to their interests through choosing a number of their school subjects. The neurological criteria were chosen to try to ensure that the individuals have no known neurological impairment that may impact upon their ability to complete the study.

The mean IQ, as measured using the Raven Matrices Sub Scale 1 (Raven, 1962), indicated the CDD participants (M = 10.79; SD = 1.05) had a higher IQ than the CDO (M = 8.71; SD=1.50). These differences represent a large effect size (D = 1.82) which mirrors previous research demonstrating lower IQ in UK offenders compared to general population (Hayes, Shackell, Mottram, & Lancaster, 2007). Both CDO and CDD participants demonstrated good basic digital skills (CDO mean = 50.00, SD = 0.00; CDD mean = 50.0, SD = 0.00) and advanced digital skills (CDO mean = 46.14, SD = 4.38; CDD mean = 46.62, SD = 6.259).

2.2. Measures

All participants completed a core battery of online questionnaires in which they were asked to complete demographic questions (e.g., age, sex, autism diagnosis), the Raven Matrices Set 1 measure of non-verbal IQ (Raven, 1962), the Basic and Advanced Digital Skills (BADS) questionnaire (Payne et al., 2019), and the Autism Quotient 50 (AQ-50; Baron-Cohen et al.,

2001). Motivations for engaging in cyber-dependent offending or declining to engage in cyber-depending offending were explored through further questioning.

Raven Matrices Set 1

Raven Matrices Sub Scale 1 (Raven, 1962) was completed as a brief assessment of non-verbal IQ. It consists of 12 matrices with participants selecting the correct answer from selection of eight possible responses. Set 1 draws upon all of the intellectual processes used in the full version of the test and has previously been used in research exploring autism and autistic traits (e.g., Brosnan et al., 2017). The measure demonstrates adequate validity and reliability ($\alpha = 0.78$; Chiesi et al., 2011, 2012). Scores can range from 0 to 12.

Basic and Advanced Digital Skills (BADS)

The BADS (Payne et al., 2019) is a 20-item questionnaire comprised of two subscales: (1) basic digital skills (10 items); and (2) advanced digital skills statements (10 items). The basic digital skills subscale includes statements such as, 'I know how to upload files' and 'I know how to adjust privacy settings'. The advanced digital skills subscale includes statements such as, 'I understand how encryption algorithms work' and 'I know how to use one of the scripting languages including BASH shell (e.g., Perl, Python, Ruby). Participants indicate on a five-point Likert scale (from not at all true of me to very true of me) their competence with the skill.

Autism Quotient 50 (AQ-50)

The AQ50 (Baron-Cohen et al., 2001) is a 50-item measure which asks participants to indicate their agreement with 50 statements (e.g., I tend to notice details that others do not) using a four-point Likert scale (from 'definitely agree' to 'definitely disagree'). It demonstrates good reliability ($\alpha = 0.75$-0.84; Broadbent et al., 2013) and validity (ROC = 0.78; Woodbury-Smith et al., 2005b). Scores range from 0 to 50 with higher scores indicative of higher numbers

of autistic traits. It has been proposed that a clinical cut-off of a score of 26 on the AQ-50 is suggestive of autism (Woodbury-Smith et al., 2005b).

Motivation for engaging in cyber-dependent offending

The interview schedule and questions included within the semi-structured interview for the CDO group were those found to be effective to understand the motivations for offending in previous research (Payne et al., 2019) and can be seen in Appendix 1. Five interviews were conducted over the telephone and two were conducted face to face at the University of Bath. All interviews were recorded on an encrypted and password protected Dictaphone and later transcribed verbatim. Interview lengths ranged from 6-38 minutes (mean = 15 minutes).

Motivation for declining to engage in cyber-dependent offending

The CDD group answered online questions about reasons for declining to engage in cyber-dependent offending. The five cyber-dependent criminality questions asked were: (1) Have you ever been in trouble with the Criminal Justice System (e.g., police, the National Crime Agency) as a result of your online behaviours (e.g., hacking, DDoS)?; (2) Have you ever been approached to commit a crime online?; (3) How did the person approach you (e.g., via game, chat room)?; (4) How did they try to convince you to commit the crime?; (5) Did you commit the proposed crime?; (5a.) If yes, why?; (5b.) If no, what do you think prevented you from engaging in the offence? It was possible that participants may have reported not having committed a cyber-dependent offence as they had not been caught. Question 5a was therefore a check to see if this may have been the case to ensure only those who had truly not committed a cyber-dependent offence were included within the CDD group.

2.3. Ethics

Ethical approval was obtained from the University of Bath Department of Psychology Ethics Committee. Prior to online questionnaire completion, participants completed an online consent form. Prior to each interview, verbal consent was recorded to confirm consent to

participate and for the interview to be recorded. Participants were advised of their right to withdraw up until the point of data anonymisation.

2.4. Data Analysis

To examine participants' reasons for engaging or declining from engaging in cyber-dependent offending, a thematic analysis was conducted in line with the guidance from Braun and Clarke (2006, 2013). The data were coded (by KP) at an explicit level, not looking beyond what the individual had said or written. Data were not coded according to a pre-determined framework but were coded in a data driven, inductive fashion (Braun & Clarke, 2006, 2013). Ideally, themes would occur more than once; however, the number of times a theme occurred did not influence its importance to the research (Braun & Clarke, 2006, 2013). To obtain inter-rater reliability a second coder (KM) coded approximately 30% of the data. Each coder initially coded the data independently. Each of the themes and sub-themes were then discussed and agreement within the coding was reached. Although the names of the identified themes and sub-themes sometimes differed, it was clear throughout the process that each coder shared the same underlying understanding of the theme.

To examine the role of autistic traits in the choice to offend or decline to offend, the AQ scores of the CDO and CDD groups were calculated. In line with de Winter (2013) the effect sizes were calculated to evaluate the magnitude of the difference between CDO and CDD autistic traits. Statistical analyses were not run because the effect sizes were smaller than 0.8 (de Winter, 2013).

3. Results

3.1. What are the motivations for engaging in cyber-dependent offending?

Seven main themes were identified with regards to CDOs' self-reported motivations for offending: (1) lack of understanding; (2) entertainment; (3) peer influence; (4) experience and career; (5) anonymity and risk perception; (6) life events; and (7) morals. All participants

reported multiple themes and sub-themes. Each theme (bold) and associated subthemes (bold italics) are described in detail in the text below and summarised.

Theme One: Lack of understanding

All CDO participants referred to the lack of understanding theme (n = 7) when interviewed as to their reasons for offending. Four sub-themes were identified: (1) consequences; (2) seriousness of behaviours; (3) lack of specific education about cyber and the law; and (4) impact of behaviour.

All the CDO participants referred to a lack of understanding about the ***consequences*** of their behaviours (n = 7). Many stated that they did not realise that law enforcement would become involved and did not realise how severe the punishment could be. Over half of the participants reported that they just did not understand the ***seriousness*** of the behaviours that they had engaged in (n = 4). This is illustrated below:

"Yes [knew it was illegal] but not to the extent that it was. I thought it was a bit shady but I didn't think it was that serious, but it was."

[Participant 1]

Throughout the interviews there was confusion as to the consequences and seriousness of the behaviours that they CDO's had engaged in, with over half of the participants (n = 4) identifying that they felt that there was a ***lack of specific education about cyber behaviours and their relationship to the law***. The interviews suggested that there was a difference in the degree of knowledge from no knowledge:

"Really there's no education on the sort of the legislation [the law] you know…. That you're at risk when you're on a computer"

[Participant 2]

To a limited amount of knowledge which was still insufficient to prevent the offending behaviours:

"So I might have not realised that it was illegal to actually own it [software] … I think I knew it would be illegal to use it on other people without their consent …"

[Participant 4]

Majority of the CDO participants did not understand the ***impact*** that their behaviour would have. Many referred to a lack of understanding in reference to people they knew (e.g., family, friends and school staff but some also referred to those who were directly impacted by their behaviour (i.e., the victims) as illustrated below:

"It's very different to a real crime when you mug someone or something … it's … you're not…..it seems victimless but its not, you know…It doesn't seem like you're hurting someone else in that sense. It sort of removes that physical element…. And so it's hard to sort of say because it just still doesn't seem kind of real that it can happen…

[Participant 2]

Theme Two: Entertainment

All participants (n = 7) mentioned an element of entertainment as a reason for engaging in the offending behaviours. The CDO's reported engaging in the behaviours because they enjoyed them rather than a need to. No participants reported engaging in behaviours with the malicious intent to commit crime:

"I was just messing around really and seeing how and why other people could do it. So it was just gaining knowledge really. That was the intent. I wouldn't say the sole intent was commit further crimes with it"

[Participant 7]

The CDO's indicated that they were inquisitive and enjoyed the ***challenge*** (n = 5) that the online environment provided:

"it's sort of a mind-set you know… if it's there it can be broken … it's sort of … a challenge … it's like … it's just something fun you know, being able to break into something like that.

It's just interesting … not many people get to see that side of it and you just learn a lot from it as you do it"

[Participant 2]

The ***curiosity*** (n = 5) that the online illegal environment provided for the CDO's was also a key motivator for many of the CDO's:

"I was quite arrogant in just doing it [the offence] because I was just curious to see if I could do it"

[Participant 1]

"I remember testing it … like on my own computers and stuff and like telling my mates in the school playground about how cool it was … but I think it was just purely curiosity honestly."

[Participant 4]

Theme Three: Peer Influence

The majority of participants (n = 6) referred to the peer influence theme. Three subthemes were identified: (1) Negative influence of peers; (2) Lack of social group; and (3) Grandiose. Participants who referenced this theme reported to be driven to offend either by the direct influence of peers, feeling isolated and/or wanting to demonstrate skill superiority over others in the cyber domain.

The ***negative influence of peers*** (n = 4) referred to the effect that others had either in an online group setting:

"the website I owned … it was a small community but we shared ideas … you know … different methods … attacks … types … techniques … and we shared with each other…

[Participant 6]

Or on an individual online setting:

"I knew a Russian hacker when I was like 12 who gave me a list of about 20,000 steam accounts that he'd hacked and he'd hacked like an actual steam admin computer so he could log loads of info and things"

[Participant 7]

However, a couple of participants also referred to a ***lack of social group*** (n = 2) as a precursor to their offending behaviours. This was in reference to offline social groups with individuals implying that they retreated online as a result of this.

"I also lost contact with some of my social circles. Coz I used to be … I used to go out with friends you know … on an everyday occurrence … but slowly you know … after college and university … I stopped for some reason … and I kinda distanced myself from … social interaction"

[Participant 6]

"…it sort of built up over a long period of time coz I was quite introverted around school … I was … I would say that I was minorly bullied but not severely bullied and it kind of made it so … erm … I didn't have as much of a social life or care as much about having a social life"

[Participant 7]

Statements indicating ***grandiose*** were made by over half of the interviewees (n = 4) with participants identifying the need to bombastically demonstrate that they had better skills than others for no other reason than to prove that they were better. This was in reference to both offline peers:

"Yeah, well we all [the group of friends from school] do computing and we're all sort of…tech savvy… and like…. I was the only one who knew how to boot someone offline"

[Participant 5]

As well as online peers:

"to …be able to hack things gives you almost a power in your mind you know… like you feel like you're slightly above than people online"

[Participant 7]

Theme Four: Experience and career

The fourth theme of experience and career was mentioned by over half of the participants (n = 4) as a motivation for engaging in cyber-dependent offending. A number of CDO's stated that they had a ***long-standing cyber interest*** (n = 3):

"I mean … I've sort of always been interested in computers and … sort of … it's sort of a mind-set you know …"

[Participant 2]

A number of interviewees also mentioned a ***desire to improve skills & pursue a cyber career*** (n = 3). CDO's recognised that they needed to engage with education to improve their skills to enable them to pursue the cyber career that they desired:

"Really I just wanted to sort of better my skills and get good so that I could pursue a professional errr … You know legal career in it because it was definitely of interest to me."

[Participant 2]

Individuals were engaged in a number of educational settings including schools, universities and online courses but some felt that the courses were not offering them the full skill set that they required. In addition to recognised education routes, some individuals were seeking education in alternative places which in some cases directly led to their offending behaviours.

"I mean I was at university at the time also [studying a cyber related course] … So you know … I was doing university and it's almost like it [practising hacking in the real world] was a different but obviously it was like an illegal course."

[Participant 6]

In addition to the perceived inadequate skills being taught, a number of the CDO's reported that they felt there was a ***lack of appropriate teaching methods or resources*** (n = 2). This was felt to be in relation to both the pedagogical methods:

"what … I did or was doing erm ... You know I couldn't have learnt that … as in at college or a university … what I was doing. So, it's sort of … giving me yeah it's … It was like a really great learning experience …"

[Participant 6]

and the engagingness of the methods offered. Participants reported finding the illegal learning environments to be more stimulating and motivating than the legal alternatives offered in school, university or via legal online training providers:

"… so yeah its [illegal activity] just sort of a way I test my skills because you know like virtual machines and like deliberately vulnerable servers they're not as fun as actually deploying it in the real world"

[Participant 2]

Some participants reported that they wanted to be taught, learn and practise their skills in a real-world environment which they had not been available to them through legal education channels. There was a ***desire for applied experience*** (n = 2):

"the experience [hacking; having own website] … It did really help me … it was real world experience rather than learning something from university or college … it's not something you can learn like that"

[Participant 6]

Theme Five: Anonymity and risk perception

The anonymity and risk perception theme was reported by over half of the CDO's (n = 4). Participants reported feeling that there was ***minimal perceived risk*** (n = 3) at the time

of offending. They reported feeling that there was a negligible risk that they would be caught and they didn't realise how easy it was for law enforcement to identify and pursue them.

"so I knew it was wrong and I knew … Like I knew there was some law against it but I didn't know … errr ... how easy it was for you to get caught I guess … so I sort of took the risk and did it …"

[Participant 5]

Participants often reported feeling this way because they had engaged in similar behaviours previously without being caught or without there being any consequences. There appeared to be an element of escalation whereby when there were no consequences for less serious behaviours, more serious illegal behaviours occurred:

"some things I've done in the past, like exploiting games, deleting games and all this … not so serious stuff I've got away with"

[Participant 7]

Aside from the element of risk, a number of participants report the feeling of ***perceived anonymity*** (n = 3). Participants felt that they could have avoided identification if they had taken steps to protect their identity:

"but they won't be able to catch everyone because only stupid people (aka me) bought it with PayPal whereas if I had bought the program with bitcoin it wouldn't be traceable with me which a lot of people have done, probably.

[Participant 7]

Aside from perceived anonymity, CDO's identified the ***importance of detachment*** (n = 2) as preceding their offending. They felt that unlike traditional crime where offenders are typically in the physical presence of the victim or their belongings, the detachment from the victim(s) helped to facilitate the offending behaviours:

"... you know you're behind a computer screen … it doesn't seem real … it doesn't seem like someone is going to come in and raid you and take your stuff … You're behind a keyboard … It's very different to a real crime when you mug someone or something … it's … you're not … it seems victimless but it's not, you know … It doesn't seem like you're hurting someone else in that sense. It sort of removes that physical element … And so it's hard to sort of say because it just still doesn't seem kind of real that it can happen …"

[Participant 2]

Theme Six: Life events

The life events theme was mentioned by a number of interviewees (n = 4). The research indicates the young age that many of the CDO's began engaging in the behaviours as well as situations or occurrences in their lives which led to the uptake and increase in illegal online behaviours.

The most commonly identified sub theme was the ***youth or immaturity*** at the time of engaging in the illegal behaviours (n = 4). Participants reported engaging in CDO behaviours from a young age:

"but if I was to start from when I was 12 it was just … exploiting things and games and then it sort of built up over a long period of time"

[Participant 7]

Some participants also referred to ***adverse life experiences*** (n = 2) which facilitated or expedited their engagement in CDO behaviours. This included growing up in dangerous neighbourhood whereby it was safer for the young person to stay indoors than to go outside:

"I was raised in a pretty erm … rough neighbourhood … if you can call it that … ******** [name of neighbourhood] … So it's quite … not the best of neighbourhoods to grow up in … you know … high crime rate and what not … Maybe that had something to do with it? ... You

know, it was safer for me to stay indoors and do the things that I was doing rather than go outside and get robbed or something."

[Participant 6]

Or having difficult living conditions at home:

"it [cyber behaviours] was also a way of you know … hacking was a way of dealing with my situation [difficult childhood/home situation]"

[Participant 6]

Or experiencing mental health difficulties whereby escaping online and pursing interests was a ***coping strategy*** (n = 2).

"… whereas [during depressive episodes] I'd go online find playing games and experimenting with hacking was the reason that I'd get up"

[Participant 7]

Theme 7: Morals

One participant provided a more nuanced motivation for engaging in CDO behaviours. His reasons for offending focussed heavily on the morals of his behaviour. He spoke about trying to do the right thing and provided a tirade of ***reasoning*** for his behaviours:

"The company kind of annoyed me in the fact that they wouldn't take responsibility for the vulnerability [the offender had rung them to tell them about the vulnerability he had found in their system before publishing their customer database which he had been able to access due to the vulnerability]"

[Participant 3]

The CDO attempted to provide some ***damage limitation***. Despite publishing the company's entire customer database, he tried to ensure that no sensitive customer data was leaked into the public domain***:***

"We sensitised the document [entire customer database] so that no sensitive information was

leaked”

[Participant 3]

Theme	Sub-theme	P1	P2	P3	P4	P5	P6	P7	Sub-theme total	AQ-50 mean (range) for each sub-theme
Lack of understanding (n = 7)	Consequences	X	X	X	X	X	X	X	7	18.29 (9-29)
	Seriousness of actions	X		X	X	X		X	4	16.6 (9-24)
	Lack of specific education regarding cyber & the law		X	X	X	X			4	15.75 (9-24)
	Impact of behaviour	X	X	X		X		X	5	18 (14-24)
Entertainment (n = 7)	Challenge		X	X		X	X	X	5	19.6 (14-29)
	Curiosity	X		X	X		X	X	5	19.6 (9-29)
Peer influence (n = 6)	Negative influence of peers	X	X			X	X		4	20 (14-29)
	Lack of social group						X	X	2	22 (15-29)
	Grandiose				X	X	X	X	4	16.75 (9-29)
Experience & career (n = 4)	Long-standing cyber interest		X		X			X	3	13.33 (9-16)
	Desire to improve skills & pursue cyber career		X				X	X	3	20 (15-29)
	Lack of appropriate teaching methods or resources		X				X		2	22.5 (16-29)
	Desire for applied experience		X				X		2	22.5 (16-29)
Anonymity & risk perception (n = 4)	Minimal perceived risk					X	X	X	3	19.33 (14-29)
	Perceived anonymity		X			X		X	3	15 (14-16(
	Importance of detachment		X				X		2	22.5 (16-29)
Life events (n = 4)	Youth or immaturity		X		X		X	X	4	17.25 (9-29)
	Adverse life experiences						X	X	2	22 (15-29)
Morals (n = 1)	Reasoning			X					1	24 (24)
	Damage limitation			X					1	24(24)

Table 2. Reported reasons for offending provided by cyber-dependent offenders with associated AQ mean scores and ranges

3.1.2. What are the motivations for declining to commit cyber-dependent offences when approached to do so?

Individuals reported that they were approached either online (e.g., via a forum, online chat room, or in-game chat) or in person to engage in cyber-dependent offending. Most CDDs provided one reason for declining, but five participants provided two reasons. From these, seven main themes were identified for declining to offend.

The first theme identified was **sticking to morals** [n = 9]. This theme suggests that some individuals choose to decline to offend because the behaviour was opposing to their ethics and their personal values. Participants stated that the proposed CDO behaviour was "against my ethics" [participant 104] and that "I stick to my principles" [participant 96].

Another identified reasons for declining to engage in CDO behaviours was the **proposed behaviour being too risky** [n = 9]. This suggests that the CDD and the CDO participants demonstrate opposing views on perceived risk and anonymity. Furthermore, in contrast to the CDO participants, the CDD participants reported having an understanding of the possible consequences of engaging in the CDO behaviours. **Being afraid of the consequences** [n = 7] was a frequent deterrent with emphasis both on the consequences that could impact the individual immediately:

"I don't want to get arrested…. I saw that other people I interacted with got arrested" [participant 158]

As well as concerns about the impact of CDO behaviour on future plans:

"future ambitions likely limited by a conviction if caught" [participant 51].

Some participants reported simply **not wanting to** [n = 3] engage in the proposed CDO behaviour or stated that they didn't offend because of **wanting to adhere to the law** [n = 3]. These reasons contrast to the CDO reasons as they demonstrate a level of understanding

about the cyber behaviours and the law. Less frequently mentioned reasons included the **behaviour being too complicated** [n = 2] suggesting the individuals do not have the required skills and the **price being too low** [n = 1] indicating the expected reward from the CDO behaviour not being great enough to warrant the behaviour.

These themes, along with the AQ scores of the CDDs who endorsed them, are presented in Table 3.

Table 3. Reasons for declining to commit proposed criminal behaviour

Theme	**n**	**Mean AQ (range)**
Sticking to morals	9	21.00 (11-33)
Proposed behaviour being too risky (e.g., being caught)	9	28.89 (11-41)
Being afraid of the consequences	7	18.71 (11-36)
Not wanting to	3	23.00 (14-38)
Wanting to adhere to the law	3	25.00 (17-29)
Behaviour being too complicated	2	37.50 (34-41)
Price being too low	1	44.00 (44)

3.2.3. Does preliminary data suggest a role for autistic traits in the decision to engage or decline to engage in cyber-dependent offending?

The data indicate that none of the CDD group and only one of the CDO reported an ASD diagnosis. The total mean AQ-50 score was higher in the CDD group than the CDO group. Table 4 provides an overview of the groups and autistic trait scores.

Table 4. Mean Autism Quotient (AQ) for the cyber-dependent decliner (CDD) and cyber-dependent offender (CDO) groups with Cohen's d statistics

	CDD group (n = 29)	CDO group (n = 7)	*D*

AQ-50 Total mean (SD)	25.10 (10.90)	18.29 (6.78)	0.66
Attention to detail mean (SD)	7.21 (2.21)	5.14 (1.57)	0.98
Attention switching mean (SD)	5.66 (2.66)	4.57 (2.07)	0.43
Communication mean (SD)	3.59 (2.90)	3.43 (2.88)	0.06
Imagination mean (SD)	3.72 (2.05)	2.29 (1.38)	0.73
Social skills mean (SD)	4.93 (3.96)	2.86 (2.34)	0.56

Tables 2 and 3 provide an overview of the motivations for engaging (table 2) or declining (table 3) to engage in CDO behaviours. Using the cut off of 26 proposed by Woodbury-Smith et al (2005), none of the reasons for engaging in CDO were associated with a mean above this score. Three themes for declining to engage in CDO were associated with a mean above 26, namely being too risky, too complicated or the price being too low. The other four themes were associated with a mean below this cut off (morals, afraid of consequences, not wanting to, being law abiding).

4. Discussion

The aims of this research were to investigate: (1) the reasons for declining to commit cyber-dependent offending when asked to offend by another person; and (2) the self-reported motivations for engaging in cyber-dependent offending and (3) the potential role of autism or autistic traits. With respect to autism, only one participant self-reported a diagnosis, and the study is therefore limited in any implications grading autism per se. The key finding relating to autistic traits was that the mean AQ-50 score for the cyber-dependent offender (CDO)

group was not only lower than the cyber-dependent declining (CDD) group but it was also lower than the proposed clinical cut-off for autism (Woodbury-Smith et al., 2005b) with a medium effect size. Potentially of interest was that for the CDD group, themes associated with an AQ score averaging above the cut off of 26 were instrumental (too risky, not enough money) whereas themes associated with an average AQ score below cut off were associated with morals/ being law abiding. This may suggest that autistic traits relate to reasons for declining to commit cyber-dependent crime and could be used to target programmes aimed at reducing cyber -dependent crime.

Approximately 17% of the non-offender sample had been approached to commit a cyber-dependent offence but had declined from doing so. Seven non-mutually exclusive reasons for declining to commit cyber-dependent crime were identified: (1) sticking to morals; (2) proposed behaviour being too risky; (3) being afraid of the consequences; (4) not wanting to; (5) wanting to adhere to the law; (6) behaviour being too complicated; and (7) price being too low. The CDOs also reported seven non-mutually exclusive reasons for engaging in offending: (1) lack of understanding; (2) entertainment; (3) peer influence; (4) experience and career; (5) anonymity and risk perception; (6) life events; and (7) morals. All CDO's reported a combination of reasons although the lack of understanding and entertainment themes were reported by all CDOs.

A comparison of the reasons for engaging and declining to commit cyber-dependent offending indicate numerous parallels which can be drawn upon to inform interventions. For example, where the non-offenders stated reasons such as being aware that the behaviour was illegal and being aware or afraid of the consequences, the offenders reported reasons which demonstrated a lack of understanding of the seriousness and consequences of their behaviour. In addition, offenders spoke of the perceived minimal risk and anonymity as well as the detachment from the victim(s) due to the cyber platform, whereas the non-offenders chose to

decline to commit offences due to a perceived high level of risk. Interventions should aim to address these reported discrepancies in understanding, and future research should investigate the preferred teaching methods to enable the intervention to have the greatest impact (e.g., whether individuals would prefer an online course, or whether this would this further increase the reported feelings of detachment from the real world). It is suggested that having CDOs that have been convicted by the Criminal Justice System (CJS) discuss their experiences of offending and the CJS (either in-person or videos) may help to address both the element of detachment as well as the perceived minimal risk of being caught and convicted.

In addition, the CDOs made several comments about changes in education. Aside from the legal side of the cyber environment they referred to changes to the way that cyber courses are taught. For example, the offenders reported engaging in illegal behaviours often due to a desire to improve their skills and apply these to the real world. One participant spoke of legal challenges requiring them to use their cyber skills (e.g., 'capture the flag' events) as being a way of improving experience of cyber education; however, many of the individuals interviewed did not appear aware of these options, highlighting the need for awareness and understanding of such events. Another possible option is the use of carefully designed labs and platforms (e.g., Immersive Labs) to enable individuals to practise their skills in a safe and legal way. Future research should look to evaluate the use of such tasks in combination with education about the law in preventing reoffending behaviours.

The current research suggests that the individuals who commit cyber-dependent offences may do so because of a lack of understanding about what is socially acceptable behaviour (i.e., legal/illegal behaviour). This is further complicated by the nature of the cyber environment which, whilst offering a wealth of opportunities, also carries many 'blurred lines' which enable individuals to cross from legal to illegal online behaviour with relatively little ease and potentially unknowingly. For example, gaming modifications are technically

breaches of copyright (i.e., illegal), however the gaming vendors frequently encourage this behaviour (CREST, 2015). Future research to objectively measure understanding of the rules governing the cyber environment in addition to an individual's ability to apply these to the cyber environment specifically (i.e., a measure of explicit social cognition specific to the cyber environment) would be helpful. This could be used to assess individuals with high cyber skills and the findings used to inform interventions to help individuals to make informed choices and prevent offending behaviours.

A number of limitations need to be acknowledged within this study. The first is the reliance on individuals to accurately report their deviant behaviours. Whilst every step was taken to reassure participants of their total anonymity and the inability to identify the individuals from their online responses, it is possible that some individuals may have under-reported their behaviours for fear of repurcussions and/or social desirability bias. Additionally, participants may have presented themselves in a way that they wish to be perceived (e.g., grandiose). A further limitation is that the current research included offenders who were known to the National Crime Agency; thus, findings may not be reflective of those who are currently unknown to the CJS (e.g., those who evade the CJS entirely). The use of only known CDOs may influence findings for a number of reasons including that they may have engaged with interventions which could have influenced how they reported their offending behaviours or even their understanding of their motivations.

Finally, the results for the motivations for offending are only tentative given the small sample size (n = 7), however data saturation was reached. Future research should be conducted with CDOs to specifically investigate whether the offenders can identify factors that either prevented further offending or would have prevented their previous offending behaviour. It would also beneficial for future research to expand upon the online questionnaires to conduct interviews with the CDD group to further explore the motivations

for not engaging in cyber-dependent offending despite being asked. This could ultimately help to inform future interventions.

Future research should investigate whether CDOs can identify factors or interventions that would have prevented their offending. The present study did not have enough participants with autism to comment upon autism per se, however it was of interest to note that overall, cyber-dependent offenders had lower autistic traits than a sample who had been approached and declined to commit from cyber-dependent offences. Clearly, the cyber-dependent offenders, had been caught which may impact upon these findings. There were suggestions that within those who declined, there were different reasons for doing so. It is speculative, but given the nature of the reasons given, it maybe that those with high autistic traits would engage in cyber-dependent crime if the rewards were high enough, where as those with lower levels of autistic traits would not. Future research can explore this potential, which would be useful for targeting future interventions to reduce cyber-dependent crime.

In conclusion, the reasons for engaging or declining to offend largely mirrored each other. For example, where the offenders reported a lack of understanding of consequences, seriousness and the law, the non-offenders reported that the awareness of these factors prevented them offending. Education appears to be the key to addressing cyber-dependent offending behaviours. This includes legal awareness through teaching, resources and safe but realistic environments for individuals to practise their skills and receive evaluation (e.g., Immersive Labs, capture the flag events).

References

Baron-Cohen, S., Hoekstra, R. A., Knickmeyer, R., & Wheelwright, S. (2006). The Autism Spectrum Quotient (AQ)—adolescent version. *Journal of Autism and Developmental Disorders, 36,* 343–350.

Baron-Cohen, S., Wheelwright, S., Skinner, R., Martin, J., & Clubley, E. (2001). The Autism-Spectrum Quotients (AQ): Evidence from Asperger Syndrome/High Functioning Autism, males and females, scientists and mathematicians. *Journal of Autism and Developmental Disorders, 31,* 5-17. https://doi.org/10.1023/A:1005653411471

Bölte, S., Westerwald, E., Holtmann, M., Freitag, C., & Poustka, F. (2011). Autistic traits and autism spectrum disorders: The clinical validity of two measures presuming a continuum of social communication skills. *Journal of Autism and Developmental Disorder, 41,* 66-72. https://doi.org/10.1007/s10803-010-1024-9

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology *Qualitative Research in Psychology. 3,* 77-101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2013). *Successful Qualitative Research: A practical guide for beginners.* London: Sage Publications Ltd.

Broadbent, J., Galic, I., & Stokes, M. A. (2013). Validation of Autism Spectrum Quotient adults version in an Australian sample. *Autism Research and Treatment*. https ://doi.org/10.1155/2013/98420 5.

Brosnan (in press). Cyber-dependent crime, autism and autistic-like traits. In Volkmar, Loftin, Westphal, & Woodbury, Smith (Eds.), *Handbook of Autism and the Law*. Springer.

Brosnan, M., & Gavin, J. (2015). *Are "Friends" Electric?.* In Rosen, L. D., Cheever, N., & Carrier, L. M. (2015). The Wiley Black Handbook of Psychology, Technology and Society. John Wiley & Sons Ltd: Chichester, UK.

Brosnan, M., Ashwin, C., & Lewton, M. (2017). Brief report: Intuitive and reflective reasoning in autism spectrum disorder. *Journal of Autism and Developmental Disorders, 47*(8), 2595–2601.

Cayubit, R. F. O., Rebolledo, K.M., Kintanar, R.G.A., Pastores, A. G., Santiago, A. J. A., & Valles, P. B. V. (2017). *Psychological Studies, 62,* 386-394. https://doi-org/10.1007/s12646-017-0423-9

Chandler, R., Russell, A. & Maras, K. L. (in press). Compliance in autism: Self-report in action. *Autism.*

Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling hackers: The science of criminal profiling as applied to the world of hacking.* Florida, USA: Taylor & Francis Group

Chiesi, F., Ciancaleoni, M., Galli, S., & Primi, C. (2012). Using the Advanced Progressive Matrices (Set I) to assess fluid ability in a short time frame: An item response theory-based analysis. *Psychological Assessment, 24,* 892–900. https ://doi.org/10.1037/a0027 830.

Chiesi, F., Primi, C., & Morsanyi, K. (2011). Developmental changes in probabilistic reasoning: The role of cognitive capacity, instructions, thinking styles, and relevant knowledge. *Thinking& Reasoning, 17,* 315–350.

Constatino, J. N., & Todd, R. D. (2003). Autistic traits in the general population: A twin study. Archives of General Psychiatry, 60, 524-530. https://doi.org.uk/10.1001/archpsyc.60.5.524

CREST. (2015). *Identify, Intervene, Inspire: Helping young people to pursue careers in cyber security, not cyber crime*. Retrieved May 11th 2018 from https://www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf

de Winter, J.C.F. (2013) "Using the Student's t-test with extremely small sample sizes," Practical Assessment, Research, and Evaluation: Vol. 18 , Article 10. DOI: https://doi.org/10.7275/e4r6-dj05

Gernsbacher, M. A., Stevenson, J. L., & Dern, S. (2017). Specificity, contexts, and reference groups matter when assessing autistic traits. *PLoS ONE 12:* e0171931. https://doi.org/10.1371/journal.pone.0171931

Hayes, S., Shackell, P., Mottram, P., & Lancaster, R. (2007). The prevalence of intellectual disability in a major UK prison. *British Journal of Learning Disabilities, 35,* 162-167. https://doi.org/10.1111/j.1468-3156.2007.00461.x

Kanne, S. M., Christ, S. E., & Reiersen, A. M. (2009). Psychiatric symptoms and psychosocial difficulties in young adults with autistic traits. Journal of Autism and Developmental Disorders, 39, 827–833.

Ledingham, R., & Mills, R. (2015). A preliminary study of autism and cybercrime in the context of international law enforcement. *Advances in Autism, 1,* 1–10. https ://doi.org/10.1108/AIA-05-2015-0003.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Retrieved 19th December 2017 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

National Crime Agency. (2016). *NCA Strategic Cyber Industry Group*. Retrieved 19th December 2017 from http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

National Crime Agency. (2017). Pathways into Cyber Crime. Retrieved 19th December 2017 from http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file

Office for National Statistics. (2017). *Crime in England and Wales: Year ending June 2017.* Retrieved 19th December 2017 from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017#latest-violent-crime-figures-continue-to-present-a-complex-picture

Payne, K., Maras., K., Russell, A. J., & Brosnan, M. J. (2020). Self-reported motivations for offending by autistic sexual offenders. *Autism, 24,* 307-320. https://doi.org.uk/10.1177/1362361319858860

Payne, K., Russell, A., Mills, R.,Maras, K., Rai, D., & Brosnan, M. (2019). Is there a relationship between cyber-dependent crime, autistic-like traits and autism?. *Journal of Autism and Developmental Disorders, 49,* 4159-4169.

Plomin, R., Haworth, C. M., & Davis, O. S. (2009). Common disorders are quantitative traits. *Nature Reviews Genetics, 10,* 872-878. https://doi.org/10.1038/nrg2670

Posserud, M. B., Lundervold, A. J., & Gillberg, C. (2006). Autistic features in a total population of 7-9 year old children assessed by the ASSQ (Autism Spectrum Screening Questionnaire). *Journal of Child Psychology and Psychiatry, 47,* 167-175.

Raven, J. C. (1962). *Advanced Raven's progressive matrices*. Melbourne: Australian Council for Educational Research.

Ronald, A., & Hoekstra, R. A. (2011). Autism spectrum disorders and autistic traits: A decade of new twin studies. *American Journal of Medical Genetics Neuropsychiatric Genetics, 156b,* 255-274. https:doi.org.uk/10.1002/ajmg.b.31159

Ruzich E, Allison C, Chakrabarti B, Smith P, Musto H, Ring H, et al. (2015b) Sex and STEM occupation predict Autism-Spectrum Quotient (AQ) scores in half a million people. *PLoS One, 10*:e0141229. https://doi.org.uk/10.1371/journal.pone.0141229

Seigfried-Spellar, K. C., O'Quinn, C. L., & Treadway, K. N. (2015). Assessing the relationship between autistic traits and cyber deviancy in a sample of college students. *Behaviour & Information Technology,* 34(5), 533-542. https://doi.org/10.1080/0144929X.2014.978377

Skuse, D., Mandy, W., Steer, C., Miller, L., Goodman, R., Lawrence, K., et al. (2009). Social communication competence and functional adaptation in a general population of children: Preliminary evidence for sex-by-verbal IQ differential risk. *Journal of the American Academy of Child and Adolescent Psychiatry, 48,* 128–137.

Sotomaa, O. (2010). When the game is not enough: Motivations and practices among computer game modding culture. *Games and Culture, 5,* 239-255. https://doi.org/ 10.1177/1555412009359765

Woodbury-Smith, M. R., Robinson, J., Wheelwright, S., & Baron-Cohen, S. (2005b). Screening adults for Asperger syndrome using the AQ: A preliminary study of its diagnostic validity in clinical practice. *Journal of Autism and Developmental Disorders,* 35, 331-335. https://doi.org/10.1080/14789940500302554

Appendix 1: Offender interview schedule exploring motivations for engaging or declining in cyber-dependent offending

1. Can you explain to me, in your own words, why you think that you committed the crime?
2. What was the main reason that you committed the crime?
    a. Are there any other reasons you think may have influenced you to commit the crime?
    b. Are these additional reasons equally important or less important?
3. Did you plan the crime?
    a. Approximately how long did you plan it for?
    b. Was it your idea?
4. Was anybody else involved in the crime (either in the planning or execution of the crime)?
    a. How many other people were involved?
    b. Whose idea was it to commit the crime?
    c. What was your role(s)?
    d. What role(s) did the other person play?
    e. Did anyone put pressure on you to commit the crime or conduct the role that you did?
5. Was the offence committed under the influence of a substance (e.g., drugs, alcohol)?
6. Did you know at the time of committing the crime that what you were about to do was illegal?
    a. Can you tell me a little more about your understanding prior to committing the crime?